



RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

melissa-store-oficial-brown.vercel.app

Objeto investigado	melissa-store-oficial-brown.vercel.app - página que se apresenta como "Melissa Oficial - Sapatos com até 97% OFF", em subdomínio gratuito da Vercel
Natureza	Verificação de vínculo com a marca declarada e de risco ao consumidor
Data da coleta	23/10/2026 (DNS, HTTP/TLS, páginas de checkout e de "taxas", catálogo JSON, base pública de CNPJ, RDAP)
Métodos	OSINT passivo · DNS · HTTP/TLS · análise do HTML e do JavaScript · validação de CNPJ
Achado central	Loja que usa a marca Melissa e o CNPJ da Grendene S.A. , vende todos os 36 modelos a R\$ 9,99 e traz no código um fluxo pós-compra de " Taxa de Logística " e " seguro " cobrados por Pix com promessa de reembolso; dados do comprador são enviados a um canal do Discord
Classificação	RISCO ALTO
Emissão do laudo	23/10/2026 as 04:31

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **melissa-store-oficial-brown.vercel.app**, realizada em **23/10/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva - requisições equivalentes às de um visitante comum e consultas a bases públicas, sem qualquer interação intrusiva, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O endereço **não é um domínio próprio**: é um subdomínio gratuito e descartável da plataforma Vercel (*.vercel.app), que qualquer pessoa cria em minutos, sem registro de titular. Ele entrega uma loja intitulada **"Melissa Oficial - Sapatos com até 97% OFF"**, com o banner "MODELOS COM MAIS DE 90% DE DESCONTO" e "Cupom TUDO9 aplicado". A Melissa é marca de calçados da **Grendene S.A.**, que a comercializa em melissa.com.br.

O catálogo, servido em products.json, tem **36 produtos - todos a R\$ 9,99**, com "preço original" entre R\$ 159,90 e R\$ 289,99, ou seja, descontos de 94% a 97%. As fotos são **capturas de tela** de outras lojas (os nomes dos arquivos trazem "Captura de tela ... cdn.shopify.com"). O rodapé exibe "© 2025 Melissa - Loja Oficial" e o **CNPJ 89.850.341/0001-60**, que, na base pública da Receita, pertence de fato à **GRENDENE S A**, ATIVA desde 1971, Sobral/CE, fabricante de calçados. O CNPJ é real - mas nada na coleta liga a Grendene a esta página. O e-mail de atendimento, contato@usarmelissabr.com, está em um domínio que **sequer está registrado** (RDAP 404 na Verisign).

O achado central está no código-fonte. O checkout coleta nome, e-mail, telefone e endereço completo e os envia a /api/capture, cuja resposta devolve um discordMessageId - isto é, **os dados do comprador são publicados num canal do Discord** a cada etapa ("started", "generated", "paid"). O pagamento é gerado por /api/pix. Depois do pagamento, o comprador é levado a upsell1.html: "O CEP informado requer uma **taxa de envio diferenciada**", "PAGAR FRETE (R\$ 9,97)", com o aviso "o valor desta taxa será **100% REEMBOLSADO**". Em seguida, upsell2.html cobra mais R\$ 9,90 por "seguro contra extravio e entrega expressa", também "100% reembolsado". E a página inicial guarda um banner de rastreio que, enquanto a primeira taxa não é paga, exibe **"PENDÊNCIA LOGÍSTICA ENCONTRADA - O envio padrão está temporariamente bloqueado"**, com o botão "LIBERAR ENVIO AGORA".

O "rastreio" não consulta transportadora alguma: os passos "Pagamento Confirmado" e "Etiqueta de Envio Gerada" são **texto fixo** no JavaScript, e o único passo variável depende de a taxa ter sido paga. É o desenho clássico de **cobranças sucessivas pós-compra**: um produto a preço irreal atrai o pagamento inicial e, em seguida, "taxas" com promessa de reembolso são apresentadas como condição para a entrega.

CLASSIFICAÇÃO DE RISCO

RISCO ALTO

Leitura: marca e CNPJ de terceiro (Grendene/Melissa) em subdomínio gratuito, preço único irreal de R\$ 9,99, e-mail em domínio inexistente, dados do comprador enviados ao Discord e **taxas pós-compra com promessa de reembolso** condicionando a entrega. Não compre e não pague nenhuma "taxa de logística" (Seções 5 e 6).

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas**. As respostas de rede e de bases públicas foram salvas no momento da coleta e tiveram hash SHA-256 calculado. O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (rdap.org / registro do gTLD / Registro.br)	rdap_raw.json

DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	dns_records.txt
Conteúdo / cabeçalhos	curl HTTPS (visitante comum), home, páginas legais e scripts	corpo_home.html · headers_home.txt · bundle_js.txt
Certificado TLS	openssl s_client / x509	tls_cert.txt
Geolocalização do IP	ipinfo.io · PTR reverso	geoip.json
CNPJ declarado	Validação por módulo 11 · base pública BrasilAPI/Receita	cnpj_publico_*.json
Consolidação	Extração de fatos e hashes SHA-256	hash_manifest.txt

3. Identificação Técnica (Domínio, DNS, Hospedagem e TLS)

Endereço	melissa-store-oficial-brown.vercel.app - subdomínio gratuito da Vercel (sem registro próprio)
Domínio-pai	vercel.app (registrado em 28/01/2020 pela Vercel; não identifica o autor da página)
DNS - A	216.198.79.66 · 64.29.17.66 (rede da Vercel) · sem MX
Servidor web	Server: Vercel · x-vercel-id gru1 (borda São Paulo)
Certificado TLS	CN=*.vercel.app (curinga da plataforma) · Google Trust Services WR1 · válido 29/08/2026-27/11/2026
Aplicação	HTML/JS estático + funções /api/capture, /api/pix, /api/status
Rastreadores	Pixel do Facebook 808181435220250 · pixel do TikTok D7JC33BC77UCM7LK8V6G
Imagens	Hospedadas em r2.paymaker.com.br - arquivos nomeados como capturas de tela de outras lojas
E-mail divulgado	contato@usarmelissabr.com - domínio não registrado (RDAP 404)
Telefone divulgado	(21) 96946-0295
CNPJ declarado	89.850.341/0001-60 - válido · GRENDENE S A · ATIVA desde 26/03/1971 · Sobral/CE · fabricação de calçados

Leitura técnica. Em um subdomínio *.vercel.app, o RDAP, o certificado e o IP descrevem a plataforma, não o autor da página - que permanece não identificado. Uma loja oficial da Grendene operaria sob domínio próprio da marca. O CNPJ exibido é o da dona real da marca, o que caracteriza **apropriação de identidade**, não indício de legitimidade. Não se imputa conduta à Vercel, à Paymaker, à Meta ou ao TikTok, meros provedores de hospedagem, armazenamento e publicidade.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

A página é um funil de venda de quatro etapas, todas no mesmo subdomínio. O código público das páginas permite reconstruí-lo sem criar pedido algum:

Etapa	O que o código faz
1. Vitrine	36 modelos Melissa a R\$ 9,99 (de R\$ 159,90-289,99), "Cupom TUDO9 aplicado", frete grátis
2. Checkout	Coleta nome, e-mail, telefone, CEP e endereço; envia a /api/capture (retorna discordMessageId) e gera Pix em /api/pix
3. upsell1.html	"Taxa de envio diferenciada" / "Taxa de Entrega Prioritária" - R\$ 9,97 por Pix, "100% REEMBOLSADO após a entrega"
4. upsell2.html	"Seguro contra extravio e entrega expressa" - R\$ 9,90 por Pix, "100% REEMBOLSADO"
Rastreio fictício	Banner "PENDÊNCIA LOGÍSTICA ENCONTRADA - envio bloqueado" até a taxa ser paga; passos de envio em texto fixo

Aspecto	Constatação
Marca usada	Melissa (Grendene S.A.) - título "Melissa Oficial", "Loja Oficial" no rodapé
Vínculo com a marca	Nenhum demonstrado - subdomínio gratuito, autor não identificado
CNPJ exibido	Da própria Grendene S.A. - apropriação de identidade
Preço	R\$ 9,99 para todos os 36 modelos (descontos de 94% a 97%)
Fotos	Capturas de tela de outras lojas
E-mail	Domínio usarmelissabr.com não registrado
Destino dos dados	Nome, e-mail, telefone e pedido enviados a um canal do Discord via /api/capture
Cobranças pós-compra	Duas "taxas" (R\$ 9,97 e R\$ 9,90) com promessa de reembolso, condicionando a entrega
Meio de pagamento	Pix gerado por /api/pix - receptor não apurado (nenhum Pix foi gerado)
Páginas legais	Itens de rodapé ("Sobre nós", "Política de Privacidade", "Trocas e Devoluções") são texto sem link; nenhuma política publicada

Leitura técnica. Lojas oficiais não enviam dados de clientes a canais de Discord, não cobram "taxa de logística" depois de confirmar o pagamento e não condicionam a entrega a um "seguro" reembolsável. A promessa de reembolso é o elemento que torna a cobrança aceitável para a vítima; o banner de "pendência logística" é o que a pressiona. Como a coleta foi passiva, não foi gerado código Pix, e o receptor dos pagamentos permanece não apurado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Fluxo pós-compra de "taxa de envio" (R\$ 9,97) e "seguro" (R\$ 9,90) com promessa de reembolso, condicionando a entrega	pag_upsell1.html · pag_upsell2.html · corpo_home.html	ALTA
2	Uso da marca Melissa e do CNPJ da Grendene S.A. sem vínculo demonstrado	corpo_home.html · cnpj_publico_89850341000160.json	ALTA
3	Dados do comprador enviados a canal do Discord a cada etapa do checkout	pag_checkout.html	ALTA
4	Todos os 36 produtos a R\$ 9,99 (descontos de 94% a 97%)	pag_products.json	ALTA

5	Rastreo fictício: etapas de envio em texto fixo e "pendência logística" atrelada à taxa	corpo_home.html	MEDIA
6	E-mail de atendimento em domínio não registrado	rdap_usarmelissabr_com.json.txt · dns_usarmelissabr_com.txt	MEDIA
7	Subdomínio gratuito da Vercel em vez de domínio da marca; fotos capturadas de outras lojas	headers_home.txt · pag_products.json	MEDIA

Síntese: 4 indicadores de severidade ALTA e 3 MEDIA. Não foi encontrado nenhum fator de legitimidade: o único dado verificável (o CNPJ) pertence à dona real da marca, sem relação demonstrada com a página.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **23/10/2026**, conclui-se que **melissa-store-oficial-brown.vercel.app** apresenta **risco alto ao consumidor**. A página usa a marca Melissa e o CNPJ da Grendene S.A. sem qualquer vínculo demonstrado, em subdomínio gratuito e de autor não identificado, vende todo o catálogo a R\$ 9,99, divulga e-mail em domínio inexistente, envia os dados dos compradores a um canal do Discord e contém, no próprio código, um fluxo de **cobranças pós-compra** - "taxa de envio" e "seguro" com promessa de reembolso - apresentadas como condição para a entrega, reforçado por um rastreo fictício. Nenhum elemento técnico sustenta que se trate de canal da marca.

Recomendações ao consumidor / solicitante

- **Não comprar** e não pagar nenhuma "taxa de logística", "frete diferenciado" ou "seguro" pedido depois da compra.
- Comprar Melissa apenas no site oficial da marca (melissa.com.br) ou em revendedores conhecidos.
- Quem já pagou: acionar o banco pelo **MED** (Mecanismo Especial de Devolução) do Pix imediatamente e guardar comprovantes e prints.
- Como nome, telefone e endereço foram enviados a terceiros, desconfiar de contatos posteriores por WhatsApp ou SMS cobrando "taxas" do pedido.

Recomendações de mitigação / denúncia

- Denunciar o subdomínio à Vercel (formulário de abuso da plataforma), indicando as páginas [upsell1.html](#) e [upsell2.html](#).
- Notificar a Grendene S.A. sobre o uso de sua marca e de seu CNPJ, para as medidas que entender cabíveis.
- Registrar boletim de ocorrência em caso de prejuízo e preservar este relatório e as evidências (pasta [evidencias/](#), com hashes SHA-256).

*Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do endereço na data indicada (coleta em 23/10/2026). A classificação expressa um **juízo técnico de risco** e não substitui decisão de autoridade policial, administrativa, regulatória ou judicial. Nenhum pedido foi criado e nenhum código Pix foi gerado; as conclusões sobre o fluxo de cobrança derivam do código-fonte público das páginas. A menção à Grendene S.A. descreve o uso do CNPJ dela pelo site e não lhe imputa qualquer participação. Não se imputa conduta ilícita aos provedores de infraestrutura citados (Vercel, Paymaker, Meta, TikTok).*

Anexo A - Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
bundle_js.txt (12942 bytes)	b070cf9f3cf5632b02400bc9b8e279c24ebc0c16a94a2418ad69bc4e4868aa84
cnpj_publico_89850341000160.json (5498 bytes)	2aaaf49e71e798498213fb38c5dcda2584846cd87d2e7f815aeb5ef408a32fcc

corpo_home.html (18834 bytes)	cc22dd3bd9e67185bddc7f2d6d6a81cf3e748d3a21a55b3667ffe9c87593830c
dns_records.txt (365 bytes)	b7c7eb94083f9301f1fbf3b3740c009d2f422632b95ca03683f98f6c3febfb847
dns_usarmelissabr_com.txt (100 bytes)	5dca399d8a8485a17d8e8b77c6ee86e56b890c1b4d6b74fac35bacce82991f39
geoip.json (281 bytes)	b8fb2129a78bace6b53840e2f6bad2bdec6ee730cc47c6988eaa13acbe2784bf
headers_home.txt (489 bytes)	7a2bd5cb0b89fb47b4385d21913dc52f7fdc12739164b5baeb0fb4d88d24629d
pag_checkout.html (29409 bytes)	9e70251c1395a768dbcfa29da68842563980fe5b6cc0acc6afa2a79b73c30d8a
pag_products.json (10144 bytes)	3f10a1b0a9cb98b238411d0ca01e1405472261412377ab781c2702a46db8b297
pag_upsell1.html (16011 bytes)	474cb6e000db797090d0576226902d025a4c4ad7fd0537b048be05fc5862e53b
pag_upsell2.html (12725 bytes)	ed3c022a93edb2628d3d54baebd6c6a71b14faf25248c8c3db4a3ead3710d990
rdap_raw.json (6757 bytes)	25e0fb6921d8bc501f705f936e04ecdd877567b5a3b91927aa7215c5cb9934f0
rdap_usarmelissabr_com.json.txt (123 bytes)	abc6bd0d0e770d78c1d59bcbb359bb11e851f1d740450caa338d8d56aa397c73
tls_cert.txt (301 bytes)	8fb2a163f621e12280a27f7e69dd2ee7bd1c70fb4db80fac261cc9e4f0cbd6a6

- Fim do relatório -